



201 – MISSING HEADER RECONSTRUCTION

TEAM INFORMATION

Team Name:

Barely Legal

Results Email:

[REDACTED]

Examination Time Frame:

to 10/31/08

INSTRUCTIONS

Description: Examiners must develop and document a methodology used to restore the missing header information in the files located in the **201_Missing File Header Reconstruction_Challenge2008** folder into the correct type files. The corrected files may be returned as files with the original filenames, preceded by OK_<original filename>.<proper extension> or the changes made to correct the original file (what was missing and what you entered as the correction) may be written out in full on the answer sheet.

Points will be awarded for successfully restored files, provided you supply a detailed methodology of how you derived your findings and correction.

Report the detailed explanation of your process (software or technique) used to determine the original challenge file problem and to correct that files information to the correct file type.

Total Weighted Points: 25 Total Points available per entry – Total 200 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

INTERNAL REVIEWER USE ONLY

Reviewer:

Points Awarded:

Date:

Review Period:

to

Completed: ☐ Yes

☐ No

☐ Partial

Team Barely Legal 201

Page 1 of 5 11/11/2008

REPORT OF EXAMINATION

201 – Missing Header Reconstruction

Changes made to reconstruct headers in files

Chaff_Landscape_158.gif:

Changed header

From: 61-FC-47-49-46-38-37

To: 47-49-46-38-39-61-64

Chaff_Landscape_219.bmp

Changed file extension

From: BMP

To: GIF

Changed header

From: 42-4D-36-04-0C-00-00

To: 47-49-46-38-39-61-64

Chaff_Landscape_272.gif

Changed header

From: FF-D8-2E-44-FA-64



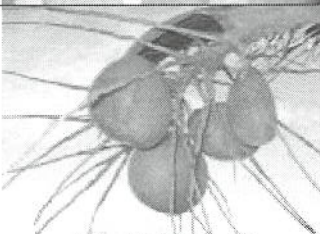
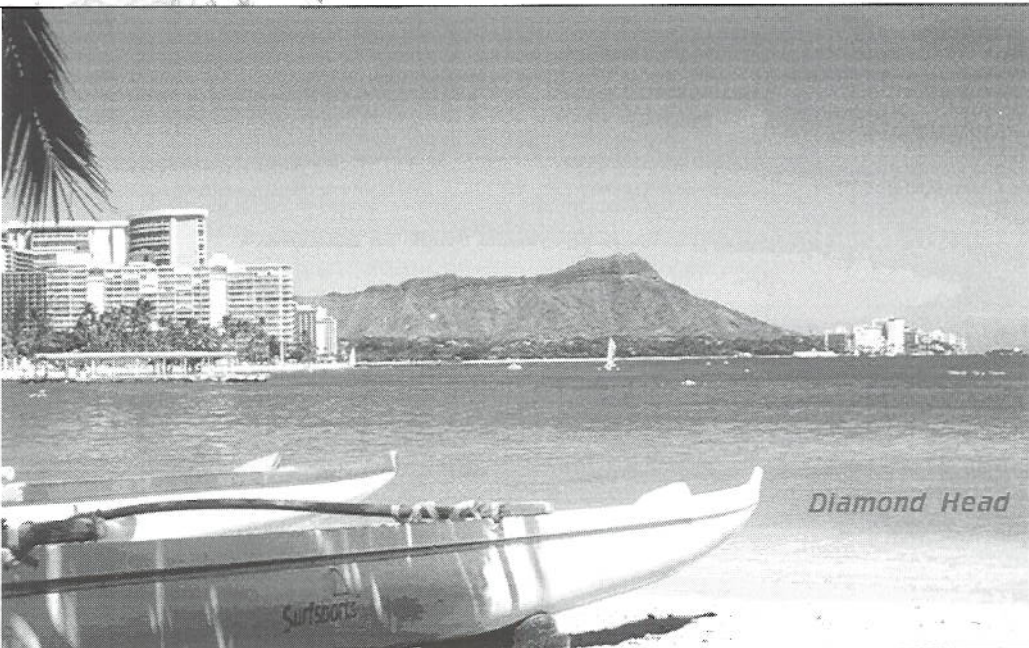
To: 47-49-46-38-39-61-64

Chaff_Buildings_625.gif

Changed header

From: 00-00-00-00-00-00-00-

To: 47-49-46-38-39-61-64

<u>Fixed File Name</u>	<u>Reconstructed Image</u>
OK_110.jpg	
OK_112.jpg	
OK_226.jpg	
OK_Chaff_Buildings_625.gif	

OK_Chaff_Landscape_158.gif



OK_Chaff_Landscape_219-BMP.gif



OK_Chaff_Landscape_272.gif



METHODOLOGY / NOTES FORM**201 - Missing File Header Reconstruction**

Date / Time	Notes
31-Oct-08 6:15 pm	<p>Tool(s) Used:</p> <p>Foremost – opensource (http://foremost.sourceforge.net/)</p> <p>Hex Workshop by BreakPoint Software (http://www.bpssoft.com/downloads/download.jsp?dlfile=hw32v514.exe)</p> <p>Used Foremost to extract thumbnail images for 110.jpg, 112.jpg, and 226.jpg</p> <p>Used Hex Workshop v5.1 (Windows) to edit and restore header information segments to these images.</p> <p>Chaff_Landscape_272-OK.gif</p> <p>Chaff_Landscape_219-BMP-OK.gif (This image also had a bad file extension)</p> <p>Chaff_Landscape_158-OK.gif</p> <p>Chaff_Buildings_625-OK.gif</p> <p>Chaff_Floral_1179-fix.gif – we believe due to the size of this file that it may be a multi-image gif file. But we were not able to restore it.</p>